PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-208922

(43)Date of publication of application : 26.07.2002

(51)Int.Cl. H04L 9/14
G09C 1/00

(21)Application number : 2001-005147

(22)Date of filing : 12.01.2001

(71)Applicant : NTT DOCOMO INC

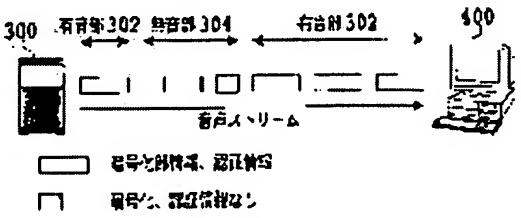
(72)Inventor : YOSHIMURA TAKESHI
SUZUKI TAKASHI
KAWAHARA TOSHIRO
EITO MINORU

(54) ENCRYPTING DEVICE, DECRYPTING DEVICE AND AUTHENTICATION INFORMATION APPLICATOR, ENCRYPTING METHOD, DECRYPTING METHOD AND AUTHENTICATION INFORMATION APPLICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an encrypting device and encrypting method which can prevent coding key and authentication key from being broken.

SOLUTION: Voice stream is transmitted from a transmission terminal 300 to a receiving terminal 400. A bit series of the voice stream includes a voice part 302 and a silent part 304. While encryption and authentication information is applied to the voice part 302, coding or authentication information is not applied to the silent part 304 and voice stream is transmitted as it is. Since encryption or authentication information is applied selectively in accordance with the kind of bit series, it is possible to prevent coding key or authentication key from being broken. Furthermore, it is also possible to reduce a throughput of encrypting processing and authentication processing and to restrain an increase of an information amount.



LEGAL STATUS

[Date of request for examination]	21.10.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開２００２－２０８９２２
(P２００２－２０８９２２A)
(43) 公開日 平成14年7月26日(2002.7.26)

(51)Int.Cl.[7]	識別記号	FI			テーマコード(参考)
H04L 9/14		G09C	1/00	640 D	5J104
G09C 1/00	640	H04L	9/00	641	

審査請求 未請求 請求項の数 17 OL (全 9 頁)

(21) 出願番号 特願2001-5147(P2001-5147)

(22) 出願日 平成13年1月12日(2001.1.12)

(71) 出願人 392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目11番1号

(72) 発明者 吉村 健
東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

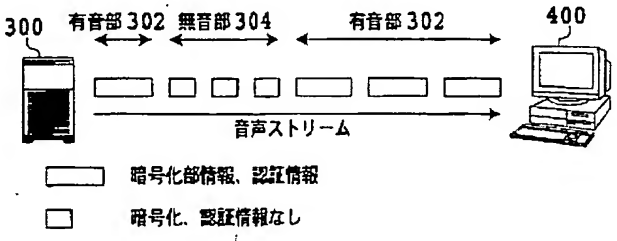
(72) 発明者 鈴木 敬
東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

(74) 代理人 100077481
弁理士 谷 義一 (外2名)

最終頁に続く

(54)【発明の名称】暗号化装置および復号装置ならびに認証情報付与装置、暗号化方法、復号方法、認証情報付与方法

(57)【要約】
【課題】 暗号鍵や認証鍵が破られるのを防ぐことができる暗号化装置および暗号化方法を提供する。
【解決手段】 送信端末３００から受信端末４００へ音声ストリームが送信されており、この音声ストリームのビット系列には、有音部３０２と、無音部３０４とが含まれている。有音部３０２には暗号化または認証情報の付与を行なう一方、無音部３０４には暗号化や認証情報の付加を行なわず、そのまま伝送する。このように、ビット系列の種類に応じて選択的に暗号化または認証情報の付与を行なうことにより、暗号鍵や認証鍵を破られることを避けることができる。また、暗号処理や認証処理の処理量を減らし、情報量の増大を抑えることができる。



1

【特許請求の範囲】

【請求項１】　送信端末から送信されるメディア情報のビット系列を暗号化して送信する暗号化装置であって、

前記ビット系列の種類を判断する判断手段と、

該判断された前記ビット系列の種類に応じて前記ビット系列の暗号化を行なう暗号化手段とを備えたことを特徴とする暗号化装置。

【請求項２】　前記ビット系列の種類は、ビット数または推定の困難性によって区別されることを特徴とする請求項１に記載の暗号化装置。

【請求項３】　前記ビット系列の種類は、暗号が解読された場合の前記メディア情報の復元の困難性によって区別されることを特徴とする請求項１に記載の暗号化装置。

【請求項４】　送信端末から送信されるビット系列を受信する受信手段と、

該受信されたビット系列が暗号化されているか否かを判断する判断手段と、

該判断の結果、前記受信されたビット系列が暗号化されていると判断された場合、前記受信されたビット系列を復号する復号手段とを備えたことを特徴とする復号装置。

【請求項５】　前記復号手段により復号されたビット系列を受信端末へ送信する送信手段を更に備えたことを特徴とする請求項４に記載の復号装置。

【請求項６】　送信端末から送信されるメディア情報のビット系列に認証情報を付与して送信する認証情報付与装置であって、

前記ビット系列の種類を判断する判断手段と、

該判断された前記ビット系列の種類に応じて前記認証情報の付与を行なう認証付与手段とを備えたことを特徴とする認証情報付与装置。

【請求項７】　前記ビット系列の種類はビット数または改竄時の影響度合いによって区別されることを特徴とする請求項６に記載の認証情報付与装置。

【請求項８】　送信端末から送信されるビット系列を受信する受信手段と、

該受信されたビット系列に認証情報が付与されているか否かを判断する判断手段と、

該判断の結果、前記受信されたビット系列に認証情報が付与されていると判断された場合、前記受信されたビット系列に基づく認証を行なう認証手段とを備えたことを特徴とする認証装置。

【請求項９】　前記認証手段による認証の結果を通知する通知手段を更に備えたことを特徴とする請求項８に記載の認証装置。

【請求項１０】　前記認証手段による認証の結果、正当であると判断されたビット系列を受信端末へ送信する送信手段を更に備えたことを特徴とする請求項８または９に記載の認証装置。

2

【請求項１１】　送信端末から送信されるメディア情報のビット系列を暗号化して送信する暗号化装置により実行される暗号化方法であって、

前記ビット系列の種類を判断する判断ステップと、

該判断された前記ビット系列の種類に応じて前記ビット系列の暗号化を行なう暗号化ステップとを備えたことを特徴とする暗号化方法。

【請求項１２】　送信端末から送信されるビット系列を復号装置により受信する受信ステップと、

該受信されたビット系列が暗号化されているか否かを判断する判断ステップと、

該判断の結果、前記受信されたビット系列が暗号化されていると判断された場合、前記受信されたビット系列を復号する復号ステップとを備えたことを特徴とする復号方法。

【請求項１３】　前記復号ステップにおいて復号されたビット系列を前記復号装置から受信端末へ送信する送信ステップを更に備えたことを特徴とする請求項１２に記載の復号方法。

【請求項１４】　送信端末から送信されるメディア情報のビット系列に認証情報を付与して送信する認証情報付与装置により実行される認証情報付与方法であって、

前記ビット系列の種類を判断する判断ステップと、

該判断された前記ビット系列の種類に応じて前記認証情報の付与を行なう認証付与ステップとを備えたことを特徴とする認証情報付与方法。

【請求項１５】　送信端末から送信されるビット系列を復号装置により受信する受信ステップと、

該受信されたビット系列に認証情報が付与されているか否かを判断する判断ステップと、

該判断の結果、前記受信されたビット系列に認証情報が付与されていると判断された場合、前記受信されたビット系列に基づく認証を行なう認証ステップとを備えたことを特徴とする認証方法。

【請求項１６】　前記認証ステップにおける認証の結果を通知する通知ステップを更に備えたことを特徴とする請求項１５に記載の認証方法。

【請求項１７】　前記認証ステップにおける認証により正当であると判断されたビット系列を復号装置から受信端末へ送信する送信ステップを更に備えたことを特徴とする請求項１５または１６に記載の認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、選択的に暗号化処理または認証処理を行なう暗号化装置および認証情報付与装置ならびに暗号化方法、復号方法、認証情報付与方法に関する。

【０００２】

【従来の技術】通信システムにおいて伝送される音声情報や画像情報等のメディア情報のビット系列をブロック

暗号を用いて暗号化する方式では、従来、たとえば図１に示すように、元のビット系列（パケット）をブロック長の整数倍に合わせるために、０ビットを付加する（パディング）。そして、パディングが行なわれたビット系列について、暗号鍵を使用してビット列の変換を行なっている。

【０００３】このようにして暗号化して送信されたビット系列は、受信側で復号鍵を使用して変換され、元のビット系列に復号される。

【０００４】また、暗号化方式を応用して認証処理を行なう場合は、図２に示すように、元のビット系列を一方向性関数で変換した値を認証鍵により暗号化した認証情報を、元のビット系列に付加して送信する。

【０００５】一方、受信側では、受信した元のビット系列に対して同一の一方向性関数を用いて求めた値を作成する。そして、作成された値と受信したビット系列を検査鍵で復号した結果との一致を判断して、受信したビット系列の送信元の正当性を確認する。

【０００６】メディア情報のビット系列についてこのような暗号処理や認証処理を行なう手法として、たとえば特開平２０００－５９３２３号公報には、重要でないデータの認証に多くの時間を要する問題を改善する技術が開示されている。この技術では、送信ユニットによりデジタルＡＶデータの重要度を判断し、その判断結果に応じて認証ルールの選択が行なわれる。

【０００７】また、特開平５－５６０３４号公報には、デジタル信号の伝送路で所定の秘匿コードに従ってデジタル信号の秘匿化を行なう技術が開示されている。この技術によれば、アナログ音声信号の無音状態を検出し、その検出結果に基づいてデジタル信号の秘匿コードを逐次変更することにより、秘匿の解読を防止する。

【０００８】

【発明が解決しようとする課題】しかしながら、上述した従来の暗号化方式または認証方式では、ビット数の少ないビット系列や容易に推定出来るビット系列に対してまで暗号化または認証処理を行なっている。このため、元のビット系列を総当りで計算すれば、容易に暗号文から平文を解読される。つまり、解読を試みる攻撃者が容易に平文と暗号文の対を入手可能であり、鍵が破られやすくなるという問題があった。

【０００９】また、送信する全てのビット系列について暗号化処理や認証処理を行なうと、オーバヘッドが増加すると共に、処理遅延が増加するという問題があった。

【００１０】また、上述した従来の暗号化方式または認証方式では、暗号化によるパディングや、認証情報の付加により、送信する情報量が増大するという問題があった。

【００１１】さらに、メディア情報の暗号化や認証に関する従来の手法では、送信するコンテンツ毎の重要度の判断処理や、秘匿コードを逐次変更する処理のために、オーバーヘッドが増大するという問題があった。

【００１２】本発明は、上記問題に鑑みてなされたものであり、その目的とするところは、暗号鍵や認証鍵が破られるのを防ぐことができる暗号化装置および認証情報付与装置ならびに暗号化方法、認証情報付与方法を提供することにある。

【００１３】また、本発明の目的は、暗号処理や認証処理のためのオーバーヘッドを軽減することができる暗号化装置および認証情報付与装置ならびに暗号化方法、認証情報付与方法を提供することにある。

【００１４】さらに、本発明の目的は、暗号化や認証情報付加による情報量の増大を抑制することができる暗号化装置および復号装置ならびに認証情報付与装置、暗号化方法、復号方法、認証情報付与方法を提供することにある。

【００１５】

【課題を解決するための手段】このような目的を達成するために、請求項１に記載の発明は、送信端末から送信されるメディア情報のビット系列を暗号化して送信する暗号化装置であって、前記ビット系列の種類を判断する判断手段と、該判断された前記ビット系列の種類に応じて前記ビット系列の暗号化を行なう暗号化手段とを備えたことを特徴とする。

【００１６】これにより、暗号鍵が破られることを防止できるとともに、暗号処理の計算量を低減することができる。また、暗号処理に伴う情報量の増大を防止することができる。

【００１７】また、請求項２に記載の発明は、請求項１に記載の暗号化装置において、前記ビット系列の種類は、ビット数または推定の困難性によって区別されることを特徴とする。

【００１８】したがって、第三者から覗かれても良いビット系列については暗号化を行なうことなくそのまま伝送することにより、暗号鍵が破られることを回避できる。

【００１９】また、請求項３に記載の発明は、請求項１に記載の暗号化装置において、前記ビット系列の種類は、暗号が解読された場合の前記メディア情報の復元の困難性によって区別されることを特徴とする。

【００２０】従って、暗号化処理に伴うオーバーヘッドやパディングによる情報量の増大を抑制することができる。

【００２１】また、請求項４に記載の発明は、復号装置であって、送信端末から送信されるビット系列を受信する受信手段と、該受信されたビット系列が暗号化されているか否かを判断する判断手段と、該判断の結果、前記受信されたビット系列が暗号化されていると判断された場合、前記受信されたビット系列を復号する復号手段とを備えたことを特徴とする。

【００２２】これにより、選択的に暗号化されたビット

系列を、そのビット系列の種類に基づいて復号することが出来る。

【００２３】また、請求項５に記載の発明は、請求項４に記載の復号装置において、前記復号手段により復号されたビット系列を受信端末へ送信する送信手段を更に備えたことを特徴とする。

【００２４】したがって、復号装置自身が受信端末である場合のみならず、受信装置とは別体の復号装置としても本発明を実施することができる。

【００２５】また、請求項６に記載の発明は、認証情報付与装置であって、送信端末から送信されるメディア情報のビット系列に認証情報を付与して送信する認証情報付与装置であって、前記ビット系列の種類を判断する判断手段と、該判断された前記ビット系列の種類に応じて前記認証情報の付与を行なう認証付与手段とを備えたことを特徴とする。

【００２６】これにより、認証鍵が破られることを防止できるとともに、認証情報付与についての計算量を低減することができる。また、認証情報付与に伴う情報量の増大を抑えることができる。

【００２７】また、請求項７に記載の発明は、請求項６に記載の認証情報付与装置において、前記ビット系列の種類はビット数または改竄時の影響度合いによって区別されることを特徴とする。

【００２８】したがって、第三者から改竄されても良いビット系列については認証情報を付与することなくそのまま伝送することにより、認証鍵が破られることを回避できる。

【００２９】また、請求項８に記載の発明は、認証装置であって、送信端末から送信されるビット系列を受信する受信手段と、該受信されたビット系列に認証情報が付与されているか否かを判断する判断手段と、該判断の結果、前記受信されたビット系列に認証情報が付与されていると判断された場合、前記受信されたビット系列に基づく認証を行なう認証手段とを備えたことを特徴とする。

【００３０】これにより、選択的に認証情報が付与されたビット系列を、そのビット系列の種類に応じて認証を行なうことが出来る。

【００３１】また、請求項９に記載の発明は、請求項８に記載の認証装置において、前記認証手段による認証の結果を通知する通知手段を更に備えたことを特徴とする。

【００３２】したがって、認証確認以降パケットそのものを処理せず、単に認証結果が正当であるかどうかのみを通知することが可能となる。

【００３３】また、請求項１０に記載の発明は、請求項８または９に記載の認証装置において、前記認証手段による認証の結果、正当であると判断されたビット系列を受信端末へ送信する送信手段を更に備えたことを特徴とする。

【００３４】したがって、認証装置自身が受信端末である場合のみならず、受信装置とは別体の認証装置としても本発明を実施することができる。

【００３５】また、請求項１１に記載の発明は、送信端末から送信されるメディア情報のビット系列を暗号化して送信する暗号化装置により実行される暗号化方法であって、前記ビット系列の種類を判断する判断ステップと、該判断された前記ビット系列の種類に応じて前記ビット系列の暗号化を行なう暗号化ステップとを備えたことを特徴とする。

【００３６】また、請求項１２に記載の発明は、復号方法であって、送信端末から送信されるビット系列を復号装置により受信する受信ステップと、該受信されたビット系列が暗号化されているか否かを判断する判断ステップと、該判断の結果、前記受信されたビット系列が暗号化されていると判断された場合、前記受信されたビット系列を復号する復号ステップとを備えたことを特徴とする。

【００３７】また、請求項１３に記載の発明は、請求項１２に記載の復号方法において、前記復号ステップにおいて復号されたビット系列を前記復号装置から受信端末へ送信する送信ステップを更に備えたことを特徴とする。

【００３８】また、請求項１４に記載の発明は、送信端末から送信されるメディア情報のビット系列に認証情報を付与して送信する認証情報付与装置により実行される認証情報付与方法であって、前記ビット系列の種類を判断する判断ステップと、該判断された前記ビット系列の種類に応じて前記認証情報の付与を行なう認証付与ステップとを備えたことを特徴とする。

【００３９】また、請求項１５に記載の発明は、認証方法であって、送信端末から送信されるビット系列を復号装置により受信する受信ステップと、該受信されたビット系列に認証情報が付与されているか否かを判断する判断ステップと、該判断の結果、前記受信されたビット系列に認証情報が付与されていると判断された場合、前記受信されたビット系列に基づく認証を行なう認証ステップとを備えたことを特徴とする。

【００４０】また、請求項１６に記載の発明は、請求項１５に記載の認証方法において、前記認証ステップにおける認証の結果を通知する通知ステップを更に備えたことを特徴とする。

【００４１】さらに、請求項１７に記載の発明は、請求項１５または１６に記載の認証方法において、前記認証ステップにおける認証により正当であると判断されたビット系列を復号装置から受信端末へ送信する送信ステップを更に備えたことを特徴とする。

【００４２】

【発明の実施の形態】以下、図面を参照し、本発明の実

施形態について詳細に説明する。

【００４３】（第１実施形態）図３は、本発明を適用した通信システムに使用される暗号化／認証付与装置の構成の一例を示す図であり、本発明に関係する部分のみを概念的に示している。

【００４４】本実施形態に係る暗号化／認証付与装置１００は、送信端末に組み込まれていても良く、送信端末とは別体として構成されても良い。また、暗号化／認証付与装置１００は、送信端末と受信端末との間に位置する無線基地局等の各ノードとして構成されても良い。

【００４５】暗号化／認証付与装置１００は、送信端末から送信するメディア情報のビット系列に対する暗号化、または認証情報の付与を選択する暗号・認証選択部１０２と、ビット系列の暗号化を行なう暗号化部１０４と、ビット系列に認証情報を付与する認証付与部１０６とから構成される。

【００４６】暗号・認証選択部１０２では、送信端末から送信するビット系列の種類が判断され、暗号化を行なうものと判断された場合、当該ビット系列が暗号化部１０４へ渡される。また、認証情報を付与すべきものと判断された場合、当該ビット系列は認証付与部１０６へ渡される。判断の結果、暗号または認証を行なわないビット系列であると判断された場合は、当該ビット系列について変換処理が行なわれることなくそのまま送信される。

【００４７】なお、暗号化／認証付与装置１００は、請求項に記載の暗号化装置または認証情報付与装置として機能する。

【００４８】次に、このように構成された暗号化／認証付与装置１００の動作の一例について、図４を参照して詳細に説明する。

【００４９】本実施形態では、暗号化や認証情報の種類は、ビット数または推定の困難性によって区別され、送信するパケットの中でもビット数の少ないビット系列や容易に推定出来る特定のビット系列に対しては、暗号化や認証情報の付与は行なわない。

【００５０】図４に示す例では、送信端末３００から受信端末４００へ音声ストリームが送信されており、この音声ストリームのビット系列には、有音部３０２と、無音部３０４とが含まれている。ここで、無音部３０４には、雑音情報等が入っており、パケット長が短い。従って、この部分の暗号文を攻撃されると、容易に暗号が破られることとなる。

【００５１】そこで、有音部３０２には暗号化または認証情報の付与を行なう一方、無音部３０４には暗号化や認証情報の付加を行なわず、そのまま伝送する。この選択処理は、図３に示す暗号化／認証付与装置１００の暗号・認証選択部１０２において、送信するパケット毎に有音部であるか無音部であるかを判断することにより行なう。

【００５２】このように、ビット系列の種類に応じて選択的に暗号化または認証情報の付与を行なうことにより、暗号鍵や認証鍵を破られることを避けるとともに、オーバーヘッドの増加を抑制できる。

【００５３】（第２実施形態）本実施形態では、メディア情報のビット系列の種類は、暗号が解読された場合のメディア情報の復元の困難性によって区別され、複数のパケットのうちの一部だけが解読されても元のメディア情報の復元には難しいビット系列は暗号化を行なわない。本実施形態もまた、上述の実施形態と同様に図３に示す暗号化／認証付与装置１００を使用することができる。

【００５４】以下、図５を参照し、図３に示すように構成された暗号化／認証付与装置１００の動作の一例について詳細に説明する。

【００５５】図５（ａ）に示す例では、送信端末３００から受信端末４００へＭＰＥＧ１により動画情報を送信する。ＭＰＥＧ１では、動画像の双方向予測（未来再生画像からの逆方向予測及び過去再生画像からの順方向予測）を行なうために、Ｉピクチャ４０６、Ｐピクチャ４０２、およびＢピクチャ４０４という３つの画像タイプが規定されている。この３つの画像タイプのうち、Ｉピクチャ４０６はフレーム内符号化画像であり、この画像タイプのビット系列が攻撃を受けた場合は、容易に元のビット系列が復元される可能性がある。一方、Ｐピクチャ４０２及びＢピクチャ４０４は予測符号化画像であり、複数の動画像間の差分のデータである。したがって、このビット系列のみを解読されても、元のメディア情報を復元することは困難である。

【００５６】そこで、図３に示す暗号化／認証付与装置１００の暗号・認証選択部１０２において、送信する動画像データの画像タイプを判断する。そして、Ｉピクチャ４０６の場合は暗号化部１０４で暗号化を行なう一方、ＰピクチャＰ４０２およびＢピクチャ４０４については暗号化を行なわず、そのまま伝送する。

【００５７】このような処理を行なうことにより、暗号化処理のオーバーヘッドやパディングによる情報量の増大を抑制することができる。

【００５８】なお、本実施形態ではＭＰＥＧ１を例に挙げて説明したが、ＭＰＥＧ１と同様にＩピクチャ、Ｐピクチャ、Ｂピクチャなどの異なるピクチャタイプを使用するＭＰＥＧ２やＭＰＥＧ４についても、本発明を適用することが可能である。

【００５９】本実施形態の応用例としては、以下のものを挙げることができる。

【００６０】ファイルを複数パケットで転送する場合、図５（ｂ）に示すように、１パケットのみを暗号化して転送する。この場合、暗号化されていないパケットに含まれる情報だけでは元のファイルを復元することができない。暗号化する部分としては、例えばファイル圧縮の

ためのコンフィギュレーション情報を含むパケットが挙げられる。その場合、残りのパケットからでは当該ファイルを元どおりに伸張することが不可能である。

【００６１】また、ビット系列の種類をビット数または改竄時の影響度合いによって区別し、一部だけ改竄されても大きな影響を与えないビット系列に対しては、認証情報を付与しないように選択処理を行なう。たとえば、ユーザ情報、課金情報、コンフィギュレーション情報、映像ストリームのＩピクチャ、階層符号化ストリームのベースレイヤなどには認証情報を付与する。一方、音声ストリームの無音情報、ＰピクチャやＢピクチャ、階層符号化における上位送の画像などは、認証情報を付与しない。

【００６２】例えば、映像や音声、音響の符号化を階層化する場合、ベースレイヤだけでもある程度のメディア品質を提供することができるが、エンハンスレイヤだけでは意味がなく、ベースレイヤとエンハンスレイヤを組み合わせることによって更に高いメディア品質を提供することができる。そこで、ベースレイヤのみを暗号化する一方、エンハンスレイヤについては暗号化を行なわずにそのまま伝送する。

【００６３】階層符号化には、異なる空間解像度（ベースレイヤはＱＣＩＦ，エンハンスレイヤはＣＩＦ、など）で階層化する場合や、異なる時間解像度（ベースレイヤは１０frame/s、エンハンスレイヤは２０frame/s、など）で階層化する場合が考えられる。

【００６４】このような処理を行なうことにより、暗号化処理のオーバーヘッドやパディングによる情報量の増大を抑制することができる。

【００６５】（第３実施形態）図６は、本発明を適用した通信システムに使用される復号／認証装置の構成の一例を示す図であり、本発明に関係する部分のみを概念的に示している。

【００６６】復号／認証装置２００は、受信端末に組み込まれていても良い。また、受信端末とは別体として構成されても良い。さらに、送信端末と受信端末との間に位置する無線基地局等の各ノードとして構成されても良い。

【００６７】復号／認証装置２００は、受信したビット系列に認証情報が付与されていることを検出するための認証検出部２０２と、受信したビット系列についての認証を行なうための認証確認部２０４と、受信したビット系列が暗号化されていることを検出するための暗号検出部２０６と、受信したビット系列が暗号化されている場合に復号処理を行なうための暗号復号部２０８とから構成される。

【００６８】復号／認証装置２００によって受信されたビット系列は、認証検出部２０２において認証情報の検出が行なわれ、検出された場合は認証確認部２０４へ当該ビット系列が渡される。認証情報の検出が行なわれなかったビット系列、および認証確認部２０４において認証が認められたビット系列は、暗号検出部２０６へ渡される。暗号検出部２０６では、ビット系列が暗号化されているか否かの検出処理が行なわれる。暗号情報が含まれている場合は、受信したビット系列が暗号復号部２０８へ渡されて復号が行なわれた後、受信端末へ送信される。暗号検出部２０６において、ビット系列が暗号化されていることが認識されなかった場合は、受信したビット系列がそのまま受信端末へ渡される。

【００６９】認証検出部２０２における認証情報の検出、および暗号検出部２０６における暗号化の有無の検出は、たとえばＩＰによって情報を転送する場合は、受信したデータに付加されているＩＰヘッダを参照することにより行なう。すなわち、ＩＰヘッダ内の「プロトコル」に含まれるプロトコル番号を参照して、そのビット系列が暗号化されているか、あるいは認証情報が付与されているかを知ることができる。また、ＲＴＰ(Real-time Transport Protocol)ヘッダ内の「ペイロードタイプ」により識別することも可能である。

【００７０】（第４実施形態）本実施形態では、図３の暗号化／認証付与装置１００と、図６の復号／認証装置２００とを組み合わせて使用する場合について説明する。

【００７１】送信端末１００の暗号・認証選択部１０２では、送信端末から送信するビット系列の種類が判断され、暗号化を行なうものと判断された場合、当該ビット系列が暗号化部１０４へ渡される。また、認証情報を付与すべきものと判断された場合、当該ビット系列は認証付与部１０６へ渡される。判断の結果、暗号または認証を行なわないビット系列であると判断された場合は、当該ビット系列について変換処理が行なわれることなくそのまま送信される。

【００７２】一方、復号／認証装置２００によって受信されたビット系列は、認証検出部２０２において認証情報の検出が行なわれ、検出された場合は認証確認部２０４へ当該ビット系列が渡される。認証情報の検出が行なわれなかったビット系列、および認証確認部２０４において認証が認められたビット系列は、暗号検出部２０６へ渡される。暗号検出部２０６では、ビット系列が暗号化されているか否かの検出処理が行なわれる。暗号情報が含まれている場合は、受信したビット系列が暗号復号部２０８へ渡されて復号が行なわれた後、受信端末へ送信される。暗号検出部２０６において、ビット系列が暗号化されていることが認識されなかった場合は、受信したビット系列がそのまま受信端末へ渡される。

【００７３】（他の実施形態）上述した実施形態では、図３に示す暗号化／認証付与装置１００を一例に説明したが、暗号化及び認証情報の付与の順序はこれに限定されず、たとえば図７の暗号化／認証付与装置６００に示すように、認証付与部１０６と暗号化部１０４の順序を

逆にしてもよい。

【００７４】また、上述した実施形態では、図６に示す復号／認証装置２００を一例に説明したが、認証確認および復号化の順序はこれに限定されず、たとえば図７の復号／認証装置６０２に示すように、暗号復号処理を認証処理に先立って行なうこととしても良い。

【００７５】また、認証確認以降パケットそのものを処理せず、単に認証結果が正当であるかどうかだけを通知することとしても良い。たとえば、図８（ａ）に示すように復号／認証装置２００が受信端末８０２に組み込まれている場合、送信端末８０１から伝送されたパケットは受信アプリケーション８０３にそのまま伝送され、認証装置２００からは前記認証手段による認証の結果（たとえば受信されたビット系列が正当である場合、その旨）を通知する。この通知処理は、図８（ｂ）に示すように復号／認証装置２００が受信端末８０２と別体として構成されている場合には、復号／認証装置２００から受信端末８０２に対して通知を行なうことにより実現できる。

【００７６】以上述べた形態以外にも、種々の変形が可能である。しかしながら、その変形が特許請求の範囲に記載された技術思想に基づくものである限り、その変形は本発明の技術範囲内となる。

【００７７】

【発明の効果】以上説明したように、本発明によれば、暗号鍵や認証鍵が破られることを防ぐことができ、通信システムにおけるデータ通信の安全性を向上することができる。

【００７８】また、メディア情報の重要性の判断のような複雑な処理を行なわず、パケット毎に選択的に暗号処理や認証処理を行なうため、従来の暗号処理や認証処理に必要であった計算量を低減することができる。結果として、オーバーヘッドを減少し、また処理遅延を回避できる。

【００７９】さらに、暗号化におけるパディングや認証情報の付加による情報量の増大を抑制することができる。

【図面の簡単な説明】

【図１】従来の暗号化の処理手順の一例を示す図である。

【図２】従来の認証情報付与の処理手順の一例を示す図である。

【図３】本発明の一実施形態に係る暗号化／認証付与装置の構成の一例を示すブロック図である。

【図４】本発明の一実施形態に係るビット系列の伝送の例を示す図である。

【図５】本発明の一実施形態に係るビット系列の伝送の例を示す図である。

【図６】本発明の一実施形態に係る復号／認証装置の構成の一例を示すブロック図である。

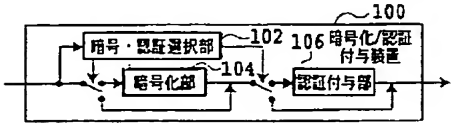
【図７】本発明の一実施形態に係る復号／認証装置の構成の一例を示すブロック図である。

【図８】本発明の一実施形態に係る、通知処理を行なう復号／認証装置の一例を示す図である。

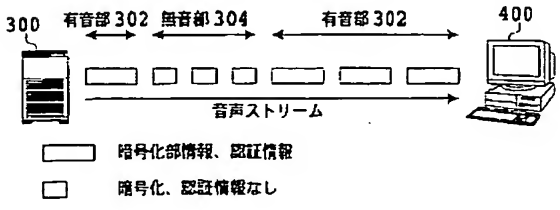
【符号の説明】

１００　暗号化／認証付与装置
１０２　暗号・認証選択部
１０４　暗号化部
１０６　認証付与部
２００　復号／認証装置
２０２　認証検出部
２０４　認証確認部
２０６　暗号検出部
２０８　暗号復号部
３００　送信端末
３０２　有音部
３０４　無音部
４００　受信端末
４０２　Ｐピクチャ
４０４　Ｂピクチャ
４０６　Ｉピクチャ
６００　暗号化／認証付与装置
６０２　復号／認証装置
８０１　送信端末
８０２　受信端末
８０３　受信アプリケーション

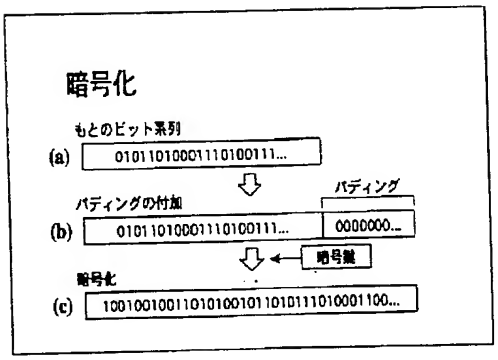
【図３】



【図４】

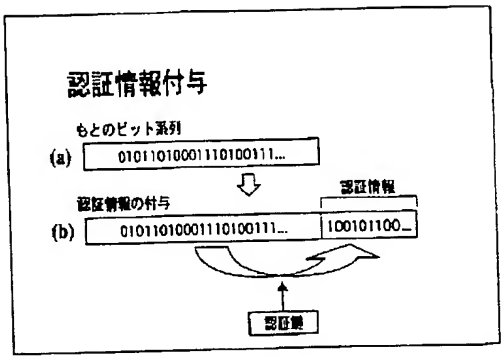


【図１】

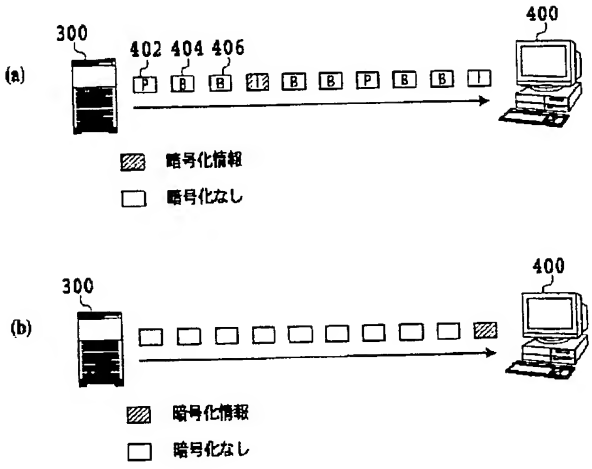


【図５】

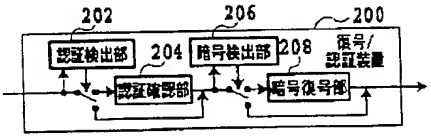
【図２】



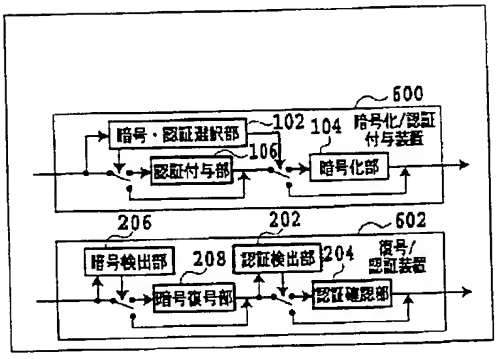
【図６】

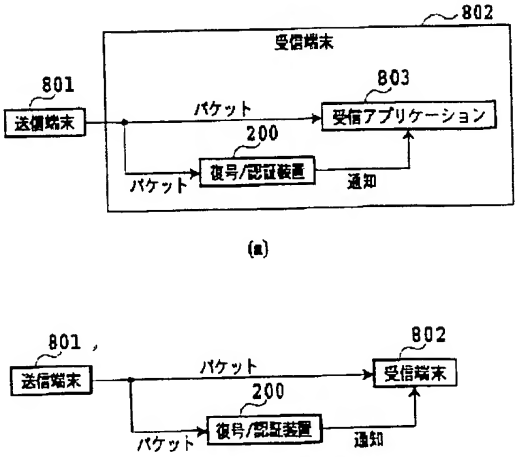


【図７】



【図８】





フロントページの続き

(72)発明者　河原　敏朗
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内

(72)発明者　栄藤　稔
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内

Ｆターム(参考)　5J104 AA01 AA33 JA03